

PALEY TYPE GROUP SCHEMES FROM CYCLOTOMIC CLASSES AND ARASU-DILLON-PLAYER DIFFERENCE SETS

YU QING CHEN AND TAO FENG

ABSTRACT. In this paper, we present constructions of abelian Paley type group schemes by using multiplicative characters of finite fields and Arasu-Dillon-Player difference sets. The constructions produce many new Paley type group schemes that were previous unknown in our classification of Paley type group schemes in finite fields of small orders.

Key words and phrases. difference set; Paley group scheme; Paley type group scheme; Paley type partial difference set; skew Hadamard difference set; Singer difference set.

Mathematics Subject Classification (2010) 05B10 05C25 05E18 05E30 .

1. INTRODUCTION

A Paley type group scheme of a finite group G is a 2-class association scheme $(G; R_0, R_1, R_2)$ obtained from a partition $D_0 = \{1\}$, D_1 , and D_2 of G such that D_1 and D_2 satisfy the equation

$$(1) \quad (1 + 2\mathbb{D}^{(-1)})(1 + 2\mathbb{D}) = |G| + (|G| - 1)G$$

in the group ring $\mathbb{Z}[G]$, where \mathbb{D} stands for the formal sum

$$\sum_{x \in \mathbb{D}} x$$

in the group ring $\mathbb{Z}[G]$ of any subset \mathbb{D} in G and the relations $R_i = \{(x, y) \in G \times G \mid xy^{-1} \in D_i\}$ for $i = 0, 1, 2$. It is easy to show that D_1 satisfies (1) if and only if D_2 satisfies (1), and therefore we will also call any subset \mathbb{D} in G that satisfies equation (1) a Paley type group scheme. Two Paley type group schemes \mathbb{D}_1 and \mathbb{D}_2 in the group G are said to be equivalent if there is an automorphism α of G such that $\mathbb{D}_2 = \mathbb{D}_1^\alpha$. Associated with each Paley type group scheme \mathbb{D} in G is a configuration $\mathfrak{C}(\mathbb{D})$ of \mathbb{D} . When $|G| \equiv 1 \pmod{4}$, a Paley type group scheme \mathbb{D} in G is also known as a Paley type partial difference set. The configuration $\mathfrak{C}(\mathbb{D})$ is the Cayley graph $\text{Cay}(G, \mathbb{D})$, which is a Paley type strongly regular graph and an example of Ramanujan graphs (see [33] for definition). When $|G| \equiv 3 \pmod{4}$, a Paley type group scheme \mathbb{D} in G is also referred to as a skew Hadamard difference set. The configuration $\mathfrak{C}(\mathbb{D})$ is the Hadamard design $\text{dev}(\mathbb{D})$ developed from \mathbb{D} (see [9]). In this paper, we study Paley type group schemes in the additive group of finite fields.

Paley type group schemes were first studied by Paley [37], who used quadratic residues in a finite field to construct Hadamard matrices. The group schemes which are equivalent to quadratic residues in a finite field will be called Paley group schemes. Automorphism groups of configurations of Paley group schemes were determined by Carlitz [10] and Kantor [30]. If we write Σ_n for the symmetric group of degree n and $\text{Gal}(\mathbb{F}_q)$ for the full automorphism group of the finite field \mathbb{F}_q of order q , then the results of Carlitz and Kantor concerning automorphism groups of configurations of Paley group schemes in [10, 30] can be summarized in the following theorem.

Theorem 1.1. [10, 30, Theorem 8.1 and Corollary 8.2] *Let q be a power of an odd prime, \mathbb{F}_q be a finite field of order q and $S_{\mathbb{F}_q}$ be the set of all non-zero quadratic residues in \mathbb{F}_q . Then*

$$\text{Aut}(\mathfrak{C}(S_{\mathbb{F}_q})) = \begin{cases} (\mathbb{F}_q \rtimes S_{\mathbb{F}_q}) \rtimes \text{Gal}(\mathbb{F}_q) & \text{if } q \notin \{3, 7, 11\}, \\ \text{PSL}(2, q) & \text{if } q \in \{7, 11\}, \\ \Sigma_3 & \text{if } q = 3. \end{cases}$$

If q is a prime, then all Paley type group schemes in \mathbb{F}_q are Paley group schemes. If q is a square of a prime, then all Paley type group schemes in \mathbb{F}_q can be constructed from partial congruence construction (see Theorem 2.2 in [34]). There are many construction methods of Paley type group schemes scattered in the literature. In [19], Davis discovered a product construction method and presented first family of Paley type group schemes in non-elementary abelian groups. Polhill [39, 40] made tremendous advances in further developing product construction methods and constructed many Paley type group schemes in abelian groups which are not of prime power orders. Peisert [38, Theorem 3.1] gave a classification of self-complementary symmetric graphs which produces a family of Paley type group schemes in $\mathbb{F}_{p^{2n}}$ for $p \equiv 3 \pmod{4}$ by using the 4-class cyclotomic amorphic group scheme. Chen [14, Theorem 3.1] also constructed a family of 4-class amorphic group schemes in \mathbb{F}_{q^4} which can be used to obtain Paley type group schemes. The discovery made by Ding and Yuan [24] re-energized research on Paley type group schemes in abelian groups of non-square orders. It is conjectured that such abelian groups must be elementary abelian p -groups and their exponent bounds were studied in [11, 15, 29, 43]. Further new discoveries were made in [23] and Paley's construction were generalized in [42] by using "quadratic residues" of commutative presemifields. Feng in [25] constructed a family of Paley type group schemes in extra-special p -groups of order p^3 and of exponent p for $p > 3$, and his construction was generalized by Chen and Polhill in [17]

using the flag group of finite fields (see [12]). In [36], Muzychuk obtained a large number of Paley type group schemes in \mathbb{F}_{q^3} and showed that the number of inequivalent such schemes grows exponentially. All results in [17, 25, 36] were generalized by Chen and Feng in [16]. In this paper we give a generalization of a cyclotomic construction of Paley type group schemes in [27] and present a new construction of Paley type group schemes in \mathbb{F}_{q^l} for odd l by using Singer difference sets, Singer relative difference sets and Arasu-Dillon-Player difference sets (see Section 2 for their definitions).

The constructions presented in this paper stem from our computer classification of Paley type group schemes in elementary abelian groups of small orders. All elementary abelian p -groups in this paper are presented as the additive group of finite fields and therefore all Paley type group schemes studied in this paper are in finite fields. By using MAGMA, we conducted exhaustive searches of all Paley type group schemes \mathbb{D} in finite fields of order ≤ 240 and classified their configurations up to isomorphism. We then compared the Paley type group schemes and their configurations with those that can be constructed from known methods and our findings are tabulated in Table 1. The finite fields of order 243 and 343 are beyond the reach of exhaustive searches. But after we imposed some symmetric conditions on \mathbb{D} , we managed to do complete searches for Paley type group schemes in these two fields that are invariant under the Galois group actions. The search results are exhibited in Table 2. The question marks in these tables indicate that there are Paley type group schemes found by computer which can not be constructed by all known methods prior to our constructions given in this paper. It is interesting that the finite field of order 243 contains so many Galois invariant Paley type group schemes, and this may only be the tip of an iceberg because there may be many non-Galois invariant Paley type group schemes since they exist in other fields. For example, By Theorem 3.2 in [27], certain unions of cosets of the subgroup of order 95 in \mathbb{F}_{113}^* are Paley type group schemes. There are, besides Paley group scheme, 5 equivalence classes of such Paley type group schemes \mathbb{D} , three of which have $|\text{Aut}(\mathfrak{C}(\mathbb{D}))| = 3 \cdot 5 \cdot 11^3 \cdot 19$, and two of which have $|\text{Aut}(\mathfrak{C}(\mathbb{D}))| = 5 \cdot 11^3 \cdot 19$. Clearly, the last two are not Galois invariant.

Throughout this paper p is an odd prime, q is a power of p , l is a positive integer, \mathbb{F} is a finite field and \mathbb{F}_q is the finite field of order q , $S_{\mathbb{F}_q}$ is the set of all non-zero quadratic residues of \mathbb{F}_q , $N_{\mathbb{F}_q}$ is the set of all quadratic non-residues of \mathbb{F}_q , \mathbb{F}_q^* is the set of all non-zero elements of \mathbb{F}_q which forms the multiplicative group of \mathbb{F}_q , $\text{Gal}(\mathbb{F}_q)$ is the full automorphism group of the field \mathbb{F}_q , and $\text{Gal}(\mathbb{F}_{q^l}/\mathbb{F}_q)$ is the Galois group of \mathbb{F}_{q^l} over \mathbb{F}_q . The main results of this paper are the following Theorems 1.2–1.4, and Theorem 1.3 is a generalization of Theorem 3.2 in [27].

Let X be a subset of the quotient group $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$, and $\pi : \mathbb{F}_{q^l}^* \rightarrow \mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ be the natural projection homomorphism. We define the subset $\mathbb{D}(X)$ in $\mathbb{F}_{q^l}^*$ to be

$$(2) \quad \mathbb{D}(X) = \{x \in S_{\mathbb{F}_{q^l}} \mid \pi(x) \in X\} \cup \{x \in N_{\mathbb{F}_{q^l}} \mid \pi(x) \notin X\}.$$

Note that when l is odd, the size $|\mathbb{D}(X)| = (q^l - 1)/2$ for all subsets X in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$.

Theorem 1.2. *Let l be an odd integer and X be a $((q^l - 1)/(q - 1), q^{l-1}, q^{l-2}(q - 1))$ -difference set in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$. Then $\mathbb{D}(X)$ is a Paley type group scheme in \mathbb{F}_{q^l} if and only if X is an Arasu-Dillon-Player difference set.*

The Paley type group schemes $\mathbb{D}(X)$ in Theorem 1.2 are $\text{Gal}(\mathbb{F}_{q^l})$ invariant when p is a strong multiplier of the Arasu-Dillon-Player difference sets X .

Theorem 1.3. *Let l be an odd integer, n be a factor of $(q^l - 1)/(q - 1)$ such that 2 is contained in the subgroup generated by p in the multiplicative group \mathbb{Z}_n^* of the modular number ring \mathbb{Z}_n , and $\gamma : \mathbb{F}_{q^l}^*/\mathbb{F}_q^* \rightarrow \mathbb{Z}_n$ be the natural projection. Then for every subset X in \mathbb{Z}_n , $\mathbb{D}(\gamma^{-1}(X))$ is a Paley type group scheme in \mathbb{F}_{q^l} .*

The Paley type group schemes in Theorem 1.3 are unions of n cyclotomic classes of order $2n$ in \mathbb{F}_{q^l} and Theorem 3.2 in [27] is an easy consequence of Theorem 1.3. Theorem 1.3 relaxed two very restrictive conditions of Theorem 3.2 in [27], namely, the number n in Theorem 1.3 does not have to

TABLE 1. Paley type group schemes \mathbb{D} that are not Paley in finite fields \mathbb{F} of order ≤ 240

$ \mathbb{F} $	Number of inequivalent \mathbb{D} and $\mathfrak{C}(\mathbb{D})$	$ \text{Aut}(\mathfrak{C}(\mathbb{D})) $	Construction methods
49	1	$2^3 \cdot 3^2 \cdot 7^2$	[19, Theorem 3.4],[38, Theorem 3.1]
81	1	$2^5 \cdot 3^5 \cdot 5$	[14, Theorem 3.1],[38, Theorem 3.1]
	1	$2^3 \cdot 3^5$?
	1	$2^7 \cdot 3^4$	[19, Theorem 3.4],[34, Theorem 2.2]
121	1	$2 \cdot 5^2 \cdot 11^2$	[19, Theorem 3.4],[34, Theorem 2.2]
	1	$2^2 \cdot 3 \cdot 5 \cdot 11^2$	[38, Theorem 3.1],[34, Theorem 2.2]
	1	$2^3 \cdot 5 \cdot 11^2$	[34, Theorem 2.2]
125	2	$2^3 \cdot 3 \cdot 5^4$	[16, Theorem 1.5]
	1	$2^3 \cdot 3 \cdot 5^3$?
169	1	$2^3 \cdot 3^2 \cdot 13^2$	[19, Theorem 3.4],[34, Theorem 2.2]
	1	$2^2 \cdot 3^2 \cdot 13^2$	[34, Theorem 2.2]
	2	$2^3 \cdot 3 \cdot 13^2$	[34, Theorem 2.2]

 TABLE 2. Non-Paley $\text{Gal}(\mathbb{F})$ invariant Paley type group schemes \mathbb{D} in finite fields \mathbb{F} of order 243 and 343

$ \mathbb{F} $	Number of inequivalent \mathbb{D} and $\mathfrak{C}(\mathbb{D})$	$ \text{Aut}(\mathfrak{C}(\mathbb{D})) $	Construction methods
243	1	$3^5 \cdot 5 \cdot 11$	[27, Theorem 3.6]
	58	$3^5 \cdot 5$?, [23, Theorem 3.3],[24, Corollary 3.7]
343	2	$3^2 \cdot 7^4$	[16, Theorem 1.5]
	2	$3^4 \cdot 7^3$?
	1	$3^3 \cdot 7^3$?
	7	$3^2 \cdot 7^3$?

be a prime power and the index $[\mathbb{Z}_n^* : \langle p \rangle]$ in Theorem 1.3 does not have to be 2. For example, since the order of 2 in $\mathbb{Z}_{7 \cdot 31}^*$ is 15, for every prime power $q \equiv 2 \pmod{7 \cdot 31}$ and every odd integer s , there are Paley type group schemes in $\mathbb{F}_{q^{15s}}$ that are unions of $7 \cdot 31$ cyclotomic classes of order $2 \cdot 7 \cdot 31$. Theorem 3.6 and Corollary 3.7 in [26] and Theorem 3.6 in [27] will also be slightly generalized in Theorem 4.5.

By using an idea in the construction of Gordon-Mills-Welch difference sets as explained by Pott [41], we obtain the following Theorem.

Theorem 1.4. *Let s and t be two positive odd integers and \tilde{R}_{q^{st}/q^t} be the $((q^{st} - 1)/(q^t - 1), (q^t - 1)/(q - 1), q^{st-t}, q^{st-2t}(q - 1))$ -Singer relative difference set in $\mathbb{F}_{q^{st}}^*/\mathbb{F}_q^*$ relative to $\mathbb{F}_{q^t}^*/\mathbb{F}_q^*$. For any subset X in $\mathbb{F}_{q^t}^*/\mathbb{F}_q^*$, $\tilde{R}_{q^{st}/q^t}^{(-1)}X$ and $\tilde{R}_{q^{st}/q^t}^{(2)}X$ are subsets in $\mathbb{F}_{q^{st}}^*/\mathbb{F}_q^*$ and if $\mathbb{D}(X)$ is a Paley type group scheme in \mathbb{F}_{q^t} , then $\mathbb{D}(\tilde{R}_{q^{st}/q^t}^{(-1)}X)$ and $\mathbb{D}(\tilde{R}_{q^{st}/q^t}^{(2)}X)$ are Paley type group schemes in $\mathbb{F}_{q^{st}}$.*

The rest of the paper is organized as follows. In Section 2, we review difference sets, relative difference sets, weighing matrices, and Singer and Arasu-Dillon-Player difference sets. In Section 3, we give a multiplicative characterization of subsets X in $\mathbb{F}_{q^t}^*/\mathbb{F}_q^*$ so that $\mathbb{D}(X)$ are Paley type group schemes in \mathbb{F}_{q^t} . Theorems 1.2–1.4 are proved in Section 4. In the concluding section, Section 5, we compare the Paley type group schemes constructed in this paper with those constructed from known methods in finite fields of small orders.

2. PRELIMINARIES ON DIFFERENCE SETS WITH SINGER PARAMETERS

In this section we review the basics of difference sets, relative difference sets, and Singer weighing matrices. We then discuss difference sets with Singer parameters. Some materials presented in this section and next section are taken from [13].

Given a finite group G of order v , a k -subset D of G is called a (v, k, λ) -difference set if for every $g \neq 1$ in G , there are exactly λ pairs of $(d_1, d_2) \in D \times D$ such that $d_1 d_2^{-1} = g$. A (v, k, λ) -difference set in a group G gives rise to a (v, k, λ) -symmetric design whose automorphism group contains G as a subgroup which acts regularly on both points and blocks of the design. If G is a group of order mn and N is a normal subgroup of G of order n , a k -subset D of G is called an (m, n, k, λ) -relative difference set relative to N if for every $g \in G \setminus N$, there are exactly λ pairs of $(d_1, d_2) \in D \times D$ such that $d_1 d_2^{-1} = g$ and there is no such expression for any $1 \neq g \in N$. An (m, n, k, λ) -relative difference set in a group G relative to a normal subgroup N of G gives rise to an (m, n, k, λ) -symmetric divisible design whose automorphism group contains G as a subgroup which acts regularly on both points and blocks of the design and the normal subgroup N is the stabilizer in G of the point classes and parallel classes of the design. when $n = 1$, an (m, n, k, λ) -relative difference set is simply an (m, k, λ) -difference set. If D is an (m, n, k, λ) -relative difference set in a group G relative to a normal subgroup N of G , an automorphism $\sigma \in \text{Aut}(G)$ such that $\{\sigma(g) \mid g \in D\} = \{gh \mid g \in D\}$ for some $h \in G$ is called a multiplier of D . Multipliers of D form a group, which will be called the multiplier group of D and will be denoted by $\mathcal{M}(D)$. Each multiplier in $\mathcal{M}(D)$ induces an automorphism of the design obtained from D . We call the subgroup $\mathcal{M}_0(D) = \{\sigma \in \text{Aut}(G) \mid \sigma(g) \in D \text{ for all } g \in D\}$ of $\mathcal{M}(D)$ the strong multiplier group of D . For more details on difference sets and relative difference sets, we refer the reader to Beth et al. [9] and Pott [41].

Let G be a finite group. The group ring $\mathbb{Z}[G]$ of the group G is the set of formal sums

$$\sum_{g \in G} a_g g,$$

where $a_g \in \mathbb{Z}$ is the integer coefficient of g in the formal sum, endowed with the addition

$$\left(\sum_{g \in G} a_g g \right) + \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} (a_g + b_g) g,$$

and multiplication

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \left(\sum_{h \in G} a_{gh^{-1}} b_h \right) g.$$

It is clear that $\mathbb{Z}[G]$ is a ring. For any subset X of G we often identify X with the group ring element

$$X = \sum_{g \in X} g$$

and for any group ring element

$$A = \sum_{g \in G} a_g g \in \mathbb{Z}[G],$$

we define $A^{(t)}$ to be

$$A^{(t)} = \sum_{g \in G} a_g g^t \in \mathbb{Z}[G]$$

for any integer $t \in \mathbb{Z}$. Using the group ring notation, a k -element subset D of G is a (v, k, λ) -difference set if and only if

$$DD^{(-1)} = (k - \lambda) + \lambda G$$

in $\mathbb{Z}[G]$, or an (m, n, k, λ) -relative difference set relative to a normal subgroup N of G if and only if

$$DD^{(-1)} = k + \lambda(G - N)$$

in $\mathbb{Z}[G]$. Let R be a ring and R^* be the multiplicative group of the invertible elements of R . If $f : G \rightarrow R^*$ is a group homomorphism, then f induces a ring homomorphism $f : \mathbb{Z}[G] \rightarrow R$ by \mathbb{Z} -linearly extending f from G to $\mathbb{Z}[G]$. Therefore for any abelian group G , every character $\chi : G \rightarrow \mathbb{C}^*$ of G can be extended to a ring homomorphism $\chi : \mathbb{Z}[G] \rightarrow \mathbb{C}$, where \mathbb{C} is the complex number field. We denote the set of all characters of G by \widehat{G} and \widehat{G} forms an abelian group under point-wise multiplication as functions from G to \mathbb{C}^* . The trivial homomorphism from G to \mathbb{C}^* is called the principal character of G . We call \widehat{G} the dual of G . By the Fourier inversion formula, one has

Lemma 2.1. *A k -element subset D of an abelian group G of order v is a (v, k, λ) -difference set if and only if for every non-principal character $\chi \in \widehat{G}$, $|\chi(D)| = \sqrt{k - \lambda}$.*

A k -element subset D of an abelian group G of order mn is an (m, n, k, λ) -relative difference set relative to a subgroup N of G of order n if and only if for every character $\chi \in \widehat{G}$ which is non-trivial on N , $|\chi(D)| = \sqrt{k}$, and for every non-principal character $\chi \in \widehat{G}$ which is trivial on N , $|\chi(D)| = \sqrt{k - \lambda n}$.

If G is an elementary abelian p -group, we can identify G with the additive group of a finite field \mathbb{F} of the same size. Let ξ_p be a primitive p -th root of unity and $\text{tr} : \mathbb{F} \rightarrow \mathbb{F}_p$ be the trace map, that is

$$\text{tr}(x) = \sum_{\sigma \in \text{Gal}(\mathbb{F})} x^\sigma$$

for all $x \in \mathbb{F}$. Then every character in $\widehat{\mathbb{F}}$ is given by

$$\begin{aligned} \chi_\alpha : \mathbb{F} &\rightarrow \mathbb{C}^* \\ \chi_\alpha(x) &= \xi_p^{\text{tr}(\alpha x)} \quad \text{for all } x \in \mathbb{F}, \end{aligned}$$

where $\alpha \in \mathbb{F}$.

In order to obtain a multiplicative description of Paley type group schemes in additive groups of finite fields, we need the Singer difference sets and Singer relative difference sets. Let $\text{tr}_{q^l/q} : \mathbb{F}_{q^l} \rightarrow \mathbb{F}_q$ be the relative trace map from \mathbb{F}_{q^l} to \mathbb{F}_q , i.e.

$$\text{tr}_{q^l/q}(x) = \sum_{\sigma \in \text{Gal}(\mathbb{F}_{q^l}/\mathbb{F}_q)} x^\sigma$$

for all $x \in \mathbb{F}_{q^l}$. Let $R_{q^l/q} = \{x \in \mathbb{F}_{q^l}^* \mid \text{tr}_{q^l/q}(x) = 1\} \subset \mathbb{F}_{q^l}^*$ and $S_{q^l/q} \subset \mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ be the image of $R_{q^l/q}$ under the natural projection map from $\mathbb{F}_{q^l}^*$ to $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$. The set $R_{q^l/q}$ is the $((q^l - 1)/(q - 1), q - 1, q^{l-1}, q^{l-2})$ -Singer relative difference set in $\mathbb{F}_{q^l}^*$ relative to \mathbb{F}_q^* . The set $S_{q^l/q}$ is the $((q^l - 1)/(q - 1), q^{l-1}, q^{l-2}(q - 1))$ -Singer difference set in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$. The complement of $S_{q^l/q}$ in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ is the $((q^l - 1)/(q - 1), (q^{l-1} - 1)/(q - 1), (q^{l-2} - 1)/(q - 1))$ -Singer difference set and it can be obtained from the projection of the hyperplane $\{x \in \mathbb{F}_{q^l}^* \mid \text{tr}_{q^l/q}(x) = 0\}$ in $\mathbb{F}_{q^l}^*$ to the quotient group $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$. The prime p is in the strong multiplier groups $\mathcal{M}_0(R_{q^l/q})$ and $\mathcal{M}_0(S_{q^l/q})$. When $l = st$ for some positive integers s and t , $R_{q^{st}/q} = R_{q^{st}/q^t} R_{q^t/q}$ as $\text{tr}_{q^{st}/q} = \text{tr}_{q^t/q} \circ \text{tr}_{q^{st}/q^t}$, and the Singer difference set $S_{q^{st}/q} = \tilde{R}_{q^{st}/q^t} S_{q^t/q}$, where \tilde{R}_{q^{st}/q^t} is the image of R_{q^{st}/q^t} under the natural projection $\mathbb{F}_{q^{st}}^* \rightarrow \mathbb{F}_{q^{st}}^*/\mathbb{F}_q^*$. We call this decomposition of $S_{q^{st}/q}$ the Gordon-Mills-Welch decomposition which forms the foundation of the Gordon-Mills-Welch construction [28] of difference sets having same

parameters as that of $S_{q^{st}/q}$. In [41], Pott presented a construction which is more general than the Gordon-Mills-Welch construction.

Proposition 2.2. [41, Proposition 3.2.1] *Let R be an (m, n, k, λ) -relative difference set in an abelian group G relative to a subgroup N , and T be an $(n/n', n', k', \lambda')$ -relative difference set in N relative to a subgroup N' of N . If $k\lambda' - k'\lambda = \lambda\lambda'(n - n')$, then the subset RT is an $(mn/n', n', kk', k\lambda')$ -relative difference set in G relative to N' .*

In [3], the following product formula for difference sets with $k - \lambda$ dividing λ was proved.

Theorem 2.3. [3, Theorem 2.3] *Let G be a group of order v and $D_1, D_2, \dots, D_{2r+1}$ be (v, k, λ) -difference sets in G with $n|\lambda$, where $n = k - \lambda$. If n^r divides $D_1 D_2 \cdots D_{2r+1}$ in $\mathbb{Z}[G]$, then there is a (v, k, λ) difference set D in G such that*

$$(3) \quad D_1 D_2 \cdots D_{2r+1} = n^r \left(\frac{k[(1 + sv)^r - 1]}{v} G + D \right) = (n + \lambda G)^r D$$

in $\mathbb{Z}[G]$, where $s = \lambda/n$.

Theorem 2.3 can also be formulated as

Theorem 2.4. *Let G be a group of order v and $D_1, D_2, \dots, D_{2r+1}$ be (v, k, λ) difference sets in G with $n|\lambda$, where $n = k - \lambda$. If $D_1 D_2 \cdots D_r$ divides $D_{r+1} D_{r+2} \cdots D_{2r+1}$ in $\mathbb{Z}[G]$, then there is a (v, k, λ) difference set D in G such that*

$$(4) \quad D_1 D_2 \cdots D_r D = D_{r+1} D_{r+2} \cdots D_{2r+1}$$

in $\mathbb{Z}[G]$.

The product formula given in equation (4) resembles in some way the non-unique factorization of algebraic integers in number fields. For instance, all $((q^l - 1)/(q - 1), q^{l-1}, q^{l-2}(q - 1))$ -difference sets satisfy the condition that $k - \lambda$ divides λ , and Arasu, Dillon and Player in [4] obtained many different factorizations of $S_{q^l/q}^{(-1)} S_{q^l/q}^{(2)}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$. These factorizations promote the following definition.

Definition 2.5. A $((q^l - 1)/(q - 1), q^{l-1}, q^{l-2}(q - 1))$ -difference set A in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ will be called an Arasu-Dillon-Player difference set if A divides $S_{q^l/q}^{(-1)} S_{q^l/q}^{(2)}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$.

Remark 2.6. There are actually several different but equivalent definitions of Arasu-Dillon-Player difference sets. For example, a $((q^l - 1)/(q - 1), q^{l-1}, q^{l-2}(q - 1))$ -difference set A in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ is an Arasu-Dillon-Player difference set if and only if $S_{q^l/q}^{(2)}$ divides $AS_{q^l/q}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$.

By Theorem 2.4, Arasu-Dillon-Player difference sets are in pairs, that is if A is an Arasu-Dillon-Player difference set in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$, then there is another Arasu-Dillon-Player difference set B in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ such that $AB = S_{q^l/q}^{(-1)} S_{q^l/q}^{(2)}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$. We will call the pair A and B a dual pair of Arasu-Dillon-Player difference sets, and call A the dual of B . The following theorem can be found in [1] and [4].

Theorem 2.7. [1, Theorem 6.17 and 6.19] *If $q^r + 1$ is prime to $(q^l - 1)/(q - 1)$, then $S_{q^l/q}^{(1+q^r)}$ is an Arasu-Dillon-Player difference set. If r is prime to l , then $S_{3^l/3}^{(\frac{1+3^r}{2})}$ is an Arasu-Dillon-Player difference set.*

We write $A_{q^l/q}(1 + q^r)$ and $A_{3^l/3}(\frac{1+3^r}{2})$ for the dual Arasu-Dillon-Player difference sets of $S_{q^l/q}^{(1+q^r)}$ and $S_{3^l/3}^{(\frac{1+3^r}{2})}$ respectively. These difference set will be used in the last section to obtain new Paley type group schemes.

Using the Gordon-Mills-Welch decomposition $S_{q^{st}/q} = \tilde{R}_{q^{st}/q^t} S_{q^t/q}$ and Proposition 2.2, one can construct more Arasu-Dillon-Player difference sets.

Theorem 2.8. *If A is a $((q^t - 1)/(q - 1), q^{t-1}, q^{t-2}(q - 1))$ -Arasu-Dillion-Player difference set in $\mathbb{F}_{q^t}^*/\mathbb{F}_q^*$, then $\tilde{R}_{q^{st}/q^t}^{(-1)}A$ and $\tilde{R}_{q^{st}/q^t}^{(2)}A$ are $((q^{st} - 1)/(q - 1), q^{st-1}, q^{st-2}(q - 1))$ -Arasu-Dillion-Player difference sets in $\mathbb{F}_{q^{st}}^*/\mathbb{F}_q^*$.*

Proof. It is easy to check that the parameters of \tilde{R}_{q^{st}/q^t} and A satisfy the condition in Proposition 2.2 with $n' = 1$. Since A is a $((q^t - 1)/(q - 1), q^{t-1}, q^{t-2}(q - 1))$ -Arasu-Dillion-Player difference set in $\mathbb{F}_{q^t}^*/\mathbb{F}_q^*$, the element A divides $S_{q^t/q}^{(-1)}S_{q^t/q}^{(2)}$ in $\mathbb{Z}[\mathbb{F}_{q^t}^*/\mathbb{F}_q^*] \subseteq \mathbb{Z}[\mathbb{F}_{q^{st}}^*/\mathbb{F}_q^*]$ and therefore both $\tilde{R}_{q^{st}/q^t}^{(-1)}A$ and $\tilde{R}_{q^{st}/q^t}^{(2)}A$ divide $\tilde{R}_{q^{st}/q^t}^{(-1)}\tilde{R}_{q^{st}/q^t}^{(2)}S_{q^t/q}^{(-1)}S_{q^t/q}^{(2)} = S_{q^{st}/q}^{(-1)}S_{q^{st}/q}^{(2)}$ in $\mathbb{Z}[\mathbb{F}_{q^{st}}^*/\mathbb{F}_q^*]$. \square

Another object that has relevance to our construction is the Singer circulant weighing matrix. Given two positive integers k and n , an $n \times n$ matrix $M = (m_{i,j})_{n \times n}$ is called a (k, n) weighing matrix if $m_{i,j}^2 = m_{i,j}$ for all $i, j = 1, 2, \dots, n$ and $MM^\top = kI_n$, where M^\top is the transpose of M and I_n is the $n \times n$ identity matrix. The set of all (k, n) weighing matrices is denoted by $W(k, n)$. An $n \times n$ matrix $M = (m_{i,j})_{n \times n}$ is said to be circulant if $m_{i',j'} = m_{i,j}$ whenever $j' - i' \equiv j - i \pmod{n}$. The set of all circulant (k, n) weighing matrices is denoted by $CW(k, n)$. Circulant matrices with integer entries can be viewed as group ring elements of a cyclic group. This is because if $M = (m_{i,j})_{n \times n}$ is a circulant matrix, let $a_i = m_{1,i+1}$ for $i = 0, 1, \dots, n-1$, $g = (g_{i,j})_{n \times n}$ with

$$g_{i,j} = \begin{cases} 1, & \text{if } j - i \equiv 1 \pmod{n} \\ 0 & \text{otherwise,} \end{cases}$$

and $G = \langle g \rangle \cong \mathbb{Z}_n$, then $M = a_0g^0 + a_1g^1 + a_2g^2 + \dots + a_{n-1}g^{n-1} \in \mathbb{Z}[G]$ and $M^\top = a_0g^0 + a_1g^{-1} + a_2g^{-2} + \dots + a_{n-1}g^{-(n-1)} = M^{(-1)} \in \mathbb{Z}[G]$. Hence a matrix $M \in CW(k, n)$ simply means that M is an element in $\mathbb{Z}[G]$ with $-1, 0, 1$ coefficients and $MM^{(-1)} = k$ in $\mathbb{Z}[G]$. Circulant weighing matrices were studied extensively in [2, 5, 6, 7, 32]. If q is a power of a prime and l is an odd positive integer, then the image R in $\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}$ of the Singer relative difference set $R_{q^l/q}$ in $\mathbb{F}_{q^l}^*$ relative to \mathbb{F}_q^* via the natural projection $\mathbb{F}_{q^l}^* \rightarrow \mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}$ is the $((q^l - 1)/(q - 1), 2, q^{l-1}, q^{l-2}(q - 1)/2)$ -Singer relative difference set in $\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}$ relative to $\mathbb{F}_q^*/S_{\mathbb{F}_q}$. The group $\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q} \cong (\mathbb{F}_{q^l}^*/\mathbb{F}_q^*) \times (\mathbb{F}_q^*/S_{\mathbb{F}_q})$. If we replace the non-trivial element of $\mathbb{F}_q^*/S_{\mathbb{F}_q} \cong \mathbb{Z}_2$ with -1 , then the relative difference set R becomes a $(q^{l-1}, (q^l - 1)/(q - 1))$ circulant weighing matrix. We call this matrix the Singer circulant weighing matrix and will denote it by $W_{q^l/q}$.

3. A MULTIPLICATIVE CHARACTERIZATION OF CERTAIN PALEY TYPE GROUP SCHEMES IN FINITE FIELDS

We now discuss a characterization of certain Paley type group schemes in finite fields by using the multiplicative group of the fields. The materials presented here are contained in [13] for $q \equiv 3 \pmod{4}$. The idea was used by Dillon in [20] and [21] for Hadamard difference sets in elementary abelian 2-groups, which is the reverse of the method used by Dillon in [22].

Definition 3.1. A subset X in $\mathbb{F}_{q^l}^*$ will be called a *projective half-point set* over \mathbb{F}_q if X is invariant under the multiplication of $S_{\mathbb{F}_q}$, i.e. X is a union of cosets of $S_{\mathbb{F}_q}$, and the intersection of X with every coset of \mathbb{F}_q^* is of size $(q - 1)/2$.

If we view $\mathbb{F}_{q^l}^*$ as the projective space $\text{PG}(l - 1, \mathbb{F}_q)$, then a coset of \mathbb{F}_q^* is a point in $\text{PG}(l - 1, \mathbb{F}_q)$ and the set X consists of half of each point in $\text{PG}(l - 1, \mathbb{F}_q)$. The following theorem gives a necessary and sufficient condition for a projective half-point set in $\mathbb{F}_{q^l}^*$ over \mathbb{F}_q to be a Paley type group scheme in \mathbb{F}_{q^l} .

Theorem 3.2. *Let D be a projective half-point set in $\mathbb{F}_{q^l}^*$ over \mathbb{F}_q . The subset D of $\mathbb{F}_{q^l}^*$ is a Paley type group scheme in the additive group of \mathbb{F}_{q^l} if and only if there is a subset \hat{D} in $\mathbb{F}_{q^l}^*$ such that D*

and \widehat{D} satisfy the equation

$$(5) \quad D^{(-1)} R_{q^l/q} = q^{(l-1)/2} \widehat{D} + \frac{q^{l-1} - q^{(l-1)/2}}{2} \mathbb{F}_{q^l}^*$$

in the group ring $\mathbb{Z}[\mathbb{F}_{q^l}^*]$, where $R_{q^l/q}$ is the $((q^l-1)/(q-1), q-1, q^{l-1}, q^{l-2})$ -Singer relative difference set in $\mathbb{F}_{q^l}^*$ relative to \mathbb{F}_q^* .

Proof. By the Fourier inversion formula, we only need to show that equation (5) is equivalent to

$$|\chi_g(1+2D)| = \sqrt{q^l}$$

for all $g \in \mathbb{F}_{q^l}^*$. The group $\mathbb{F}_{q^l}^*$ can be partitioned into three subsets

$$\begin{aligned} H^* &= \{x \in \mathbb{F}_{q^l}^* \mid \text{tr}_{q^l/q}(x) = 0\}, \\ S_{\mathbb{F}_q} R_{q^l/q} &= \{x \in \mathbb{F}_{q^l}^* \mid \text{tr}_{q^l/q}(x) \in S_{\mathbb{F}_q}\}, \\ N_{\mathbb{F}_q} R_{q^l/q} &= \{x \in \mathbb{F}_{q^l}^* \mid \text{tr}_{q^l/q}(x) \in N_{\mathbb{F}_q}\}. \end{aligned}$$

Given an element $g \in \mathbb{F}_{q^l}^*$, the character sum

$$\begin{aligned} \chi_g(1+2D) &= 1 + 2 \sum_{x \in D} \xi_p^{\text{tr}_{q^l/p}(gx)} \\ &= 1 + 2 \sum_{x \in D, gx \in H^*} \xi_p^{\text{tr}_{q^l/p}(gx)} + 2 \sum_{x \in D, gx \in S_{\mathbb{F}_q} R_{q^l/q}} \xi_p^{\text{tr}_{q^l/p}(gx)} + 2 \sum_{x \in D, gx \in N_{\mathbb{F}_q} R_{q^l/q}} \xi_p^{\text{tr}_{q^l/p}(gx)} \end{aligned}$$

with

$$\begin{aligned} 1 + 2 \sum_{x \in D, gx \in H^*} \xi_p^{\text{tr}_{q^l/p}(gx)} &= 1 + 2 \sum_{x \in D, gx \in H^*} \xi_p^{\text{tr}_{q/p}(\text{tr}_{q^l/q}(gx))} \\ &= 1 + 2|gD \cap H^*| = 1 + |H^*| = q^{l-1}, \end{aligned}$$

$$\begin{aligned} 2 \sum_{x \in D, gx \in S_{\mathbb{F}_q} R_{q^l/q}} \xi_p^{\text{tr}_{q^l/p}(gx)} &= 2 \sum_{x \in D, gx \in S_{\mathbb{F}_q} R_{q^l/q}} \xi_p^{\text{tr}_{q/p}(\text{tr}_{q^l/q}(gx))} \\ &= 2|gD \cap R_{q^l/q}| \sum_{x \in S_{\mathbb{F}_q}} \xi_p^{\text{tr}_{q/p}(x)} \\ &= 2|gD \cap R_{q^l/q}| \chi_1(S_{\mathbb{F}_q}), \end{aligned}$$

and

$$\begin{aligned} 2 \sum_{x \in D, gx \in N_{\mathbb{F}_q} R_{q^l/q}} \xi_p^{\text{tr}_{q^l/p}(gx)} &= 2 \sum_{x \in D, gx \in N_{\mathbb{F}_q} R_{q^l/q}} \xi_p^{\text{tr}_{q/p}(\text{tr}_{q^l/q}(gx))} \\ &= 2|gD \cap \omega R_{q^l/q}| \sum_{x \in N_{\mathbb{F}_q}} \xi_p^{\text{tr}_{q/p}(x)} \\ &= 2|gD \cap \omega R_{q^l/q}| \chi_1(N_{\mathbb{F}_q}), \end{aligned}$$

where ω is a primitive element in \mathbb{F}_q . Note that $|gD \cap \omega R_{q^l/q}| = |g\omega^{-1}D \cap R_{q^l/q}|$. Since $D \cap \omega^{-1}D = \emptyset$ and $D \cup \omega^{-1}D = \mathbb{F}_{q^l}^*$ as D is a projective half-point set in $\mathbb{F}_{q^l}^*$ over \mathbb{F}_q , we also have $gD \cap g\omega^{-1}D = \emptyset$ and $gD \cup g\omega^{-1}D = \mathbb{F}_{q^l}^*$ for all $g \in \mathbb{F}_{q^l}^*$. This implies that

$$(6) \quad |gD \cap R_{q^l/q}| + |gD \cap \omega R_{q^l/q}| = |gD \cap R_{q^l/q}| + |g\omega^{-1}D \cap R_{q^l/q}| = |R_{q^l/q}| = q^{l-1}.$$

Therefore D is a Paley type group scheme if and only if

$$\begin{aligned}\sqrt{q^l} &= |\chi_g(1 + 2D)| = |gD \cap R_{q^l/q}| \chi_1(1 + 2S_{\mathbb{F}_q}) + |gD \cap \omega R_{q^l/q}| \chi_1(1 + 2N_{\mathbb{F}_q})| \\ &= (|gD \cap R_{q^l/q}| - |gD \cap \omega R_{q^l/q}|) \chi_1(1 + 2S_{\mathbb{F}_q}),\end{aligned}$$

which is equivalent to

$$(7) \quad |gD \cap R_{q^l/q}| - |gD \cap \omega R_{q^l/q}| = \pm q^{\frac{l-1}{2}}.$$

Combining (6) and (7), we get

$$(8) \quad |gD \cap R_{q^l/q}| = \frac{q^{l-1} \pm q^{\frac{l-1}{2}}}{2},$$

Let

$$\widehat{D} = \{g \in \mathbb{F}_{q^l}^* \mid |gD \cap R_{q^l/q}| = \frac{q^{l-1} + q^{\frac{l-1}{2}}}{2}\} = \{g \in \mathbb{F}_{q^l}^* \mid \chi_g(1 + 2D) = q^{\frac{l-1}{2}} \chi_1(1 + 2S_{\mathbb{F}_q})\}.$$

Then

$$\omega \widehat{D} = \{g \in \mathbb{F}_{q^l}^* \mid |gD \cap R_{q^l/q}| = \frac{q^{l-1} - q^{\frac{l-1}{2}}}{2}\} = \{g \in \mathbb{F}_{q^l}^* \mid \chi_g(1 + 2D) = q^{\frac{l-1}{2}} \chi_1(1 + 2N_{\mathbb{F}_q})\}$$

and

$$\begin{aligned}D^{(-1)} R_{q^l/q} &= \frac{q^{l-1} + q^{\frac{l-1}{2}}}{2} \widehat{D} + \frac{q^{l-1} - q^{\frac{l-1}{2}}}{2} (\omega \widehat{D}) \\ &= q^{\frac{l-1}{2}} \widehat{D} + \frac{q^{l-1} - q^{\frac{l-1}{2}}}{2} \mathbb{F}_{q^l}^*\end{aligned}$$

in the group ring $\mathbb{Z}[\mathbb{F}_{q^l}^*]$. □

Remark 3.3. From the proof it is easy to see that \widehat{D} is also a projective-half point set and satisfies

$$\widehat{D}^{(-1)} R_{q^l/q} = q^{\frac{l-1}{2}} \widehat{D} + \frac{q^{l-1} - q^{\frac{l-1}{2}}}{2} \mathbb{F}_{q^l}^*$$

in the group ring $\mathbb{Z}[\mathbb{F}_{q^l}^*]$. Therefore $\widehat{D}^{(-1)}$ is also a Paley type group scheme and it is the dual of D .

The next theorem is equivalent to Theorem 3.2 but much easier to use. Its proof requires the following lemma of Ma [35].

Lemma 3.4. [35, Lamma 3.4] *Let a_1, a_2, \dots, a_m be integers and*

$$\sum_{i=1}^m a_i = n.$$

If $n = qm + r$, where q and r are integers and $0 \leq r < m$, then

$$\sum_{i=1}^m a_i^2 \geq (m-r)q^2 + r(q+1)^2$$

and equality holds if and only if $|a_i - a_j| \leq 1$ for all $1 \leq i, j \leq m$, i.e. there are exactly $m-r$ of a_1, a_2, \dots, a_m with value q and the remaining r of them with value $q+1$.

Proof. If there are i and j such that $a_i - a_j > 1$, let $a'_k = a_k$ for $k \neq i$ or j , $a'_i = a_i - 1$ and $a'_j = a_j + 1$, then

$$\sum_{k=1}^m a'_k = \sum_{k=1}^m a_k = n$$

and

$$\sum_{k=1}^m a_k'^2 = \sum_{k=1}^m a_k^2 + 2(1 + a_j - a_i) < \sum_{k=1}^m a_k^2.$$

Hence $\sum_{k=1}^m a_k'^2$ attains minimum if and only if $m - r$ of the integers a_1, a_2, \dots, a_m are equal to q and the remaining r of them are equal to $q + 1$. \square

Theorem 3.5. *A projective half-point set D in $\mathbb{F}_{q^l}^*$ over \mathbb{F}_q is a Paley type group scheme in \mathbb{F}_{q^l} if and only if $D^{(-1)}R_{q^l/q}$ is divisible by $q^{(l-1)/2}$ in the group ring $\mathbb{Z}[\mathbb{F}_{q^l}^*]$, where $R_{q^l/q}$ is the $((q^l - 1)/(q - 1), q - 1, q^{l-1}, q^{l-2})$ -Singer relative difference set in $\mathbb{F}_{q^l}^*$ relative to \mathbb{F}_q^* .*

Proof. If D is a Paley type group scheme in \mathbb{F}_{q^l} , then by Theorem 3.2, $D^{(-1)}R_{q^l/q}$ is divisible by $q^{(l-1)/2}$ in the group ring $\mathbb{Z}[\mathbb{F}_{q^l}^*]$. Conversely, if $D^{(-1)}R_{q^l/q}$ is divisible by $q^{(l-1)/2}$ in the group ring $\mathbb{Z}[\mathbb{F}_{q^l}^*]$, then

$$\frac{D^{(-1)}R_{q^l/q}}{q^{\frac{l-1}{2}}} = \sum_{g \in \mathbb{F}_{q^l}^*} a_g g \in \mathbb{Z}[\mathbb{F}_{q^l}^*]$$

for some integers a_g and

$$(9) \quad \sum_{g \in \mathbb{F}_{q^l}^*} a_g = \frac{q^{\frac{l-1}{2}}(q^l - 1)}{2} = \frac{q^{\frac{l-1}{2}} - 1}{2}(q^l - 1) + \frac{q^l - 1}{2}.$$

Since

$$\begin{aligned} D^{(-1)}R_{q^l/q}(D^{(-1)}R_{q^l/q})^{(-1)} &= DD^{(-1)}(q^{l-1} + q^{l-2}(\mathbb{F}_{q^l}^* - \mathbb{F}_q^*)) \\ &= q^{l-1}DD^{(-1)} + \frac{q^{l-2}(q^l - 1)^2}{4}\mathbb{F}_{q^l}^* - \frac{q^{l-2}(q^l - 1)(q - 1)}{4}\mathbb{F}_{q^l}^* \\ &= q^{l-1}DD^{(-1)} + \frac{q^{l-1}(q^l - 1)(q^{l-1} - 1)}{4}\mathbb{F}_{q^l}^* \end{aligned}$$

as D is a projective half-point set in $\mathbb{F}_{q^l}^*$ over \mathbb{F}_q , we find that

$$(10) \quad \sum_{g \in \mathbb{F}_{q^l}^*} a_g^2 = \frac{q^l - 1}{2} + \frac{(q^l - 1)(q^{l-1} - 1)}{4} = \left(\frac{q^{\frac{l-1}{2}} - 1}{2}\right)^2 \frac{q^l - 1}{2} + \left(\frac{q^{\frac{l-1}{2}} + 1}{2}\right)^2 \frac{q^l - 1}{2}.$$

By Lemma 3.4, there is a subset \widehat{D} of size $(q^l - 1)/2$ in $\mathbb{F}_{q^l}^*$ such that

$$\frac{D^{(-1)}R_{q^l/q}}{q^{\frac{l-1}{2}}} = \widehat{D} + \frac{q^{\frac{l-1}{2}} - 1}{2}\mathbb{F}_{q^l}^*.$$

By Theorem 3.2, D is a Paley type group scheme. \square

Let $\mu : \mathbb{F}_{q^l}^* \rightarrow \mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}$ be the natural projection map. There is an one-to-one correspondence between projective half-point sets in $\mathbb{F}_{q^l}^*$ over \mathbb{F}_q^* and transversals of $\mathbb{F}_q^*/S_{\mathbb{F}_q}$ in $\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}$. Combining Theorems 3.2, Remark 3.3 and Theorem 3.5, one has

Corollary 3.6. *Let D be a transversal of the subgroup $\mathbb{F}_q^*/S_{\mathbb{F}_q}$ in $\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}$ and R be the $((q^l - 1)/(q - 1), 2, q^{l-1}, q^{l-2}(q - 1)/2)$ -Singer relative difference set in $\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}$ relative to $\mathbb{F}_q^*/S_{\mathbb{F}_q}$. Then the following statements are equivalent:*

- (i) $\mu^{-1}(D)$ is a Paley type group scheme in the additive group of \mathbb{F}_{q^l} ;

(ii) *there is another transversal \widehat{D} of the subgroup $\mathbb{F}_q^*/S_{\mathbb{F}_q}$ in $\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}$ such that*

$$D^{(-1)}R = q^{(l-1)/2}\widehat{D} + \frac{q^{l-1} - q^{(l-1)/2}}{2}\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}$$

in $\mathbb{Z}[\mathbb{F}_{q^l}^/S_{\mathbb{F}_q}]$;*

(iii) *$D^{(-1)}R$ is divisible by $q^{(l-1)/2}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}]$.*

When l is odd, the group $\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q} \cong (\mathbb{F}_{q^l}^*/\mathbb{F}_q^*) \times (\mathbb{F}_q^*/S_{\mathbb{F}_q})$. Let $\eta_{\mathbb{F}_q^*}$ be the non-principal character of $\mathbb{F}_q^*/S_{\mathbb{F}_q}$. Then $\eta_{\mathbb{F}_q^*}$ can be extended to a ring homomorphism $\mathbb{Z}[\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}] \rightarrow \mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$, which will be again denoted by $\eta_{\mathbb{F}_q^*}$. The ring homomorphism $\eta_{\mathbb{F}_q^*}$ amounts to replace the non-identity element of $\mathbb{F}_q^*/S_{\mathbb{F}_q}$ by -1 and clearly $\eta_{\mathbb{F}_q^*}(R) = W_{q^l/q}$. Also $\eta_{\mathbb{F}_q^*}$ induces an one-to-one correspondence between transversals of $\mathbb{F}_q^*/S_{\mathbb{F}_q}$ in $\mathbb{F}_{q^l}^*/S_{\mathbb{F}_q}$ and elements in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$ with ± 1 coefficients, which we denote by $\tilde{\eta}_{\mathbb{F}_q^*}$.

Corollary 3.7. *Let l be odd, D be an element with ± 1 coefficients in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$ and $W_{q^l/q}$ be the Singer circulant weighing matrix in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$. Then the following statements are equivalent:*

- (i) *$(\tilde{\eta}_{\mathbb{F}_q^*} \circ \mu)^{-1}(D)$ is a Paley type group scheme in \mathbb{F}_{q^l} ;*
- (ii) *there is another ± 1 coefficient element \widehat{D} in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$ such that*

$$D^{(-1)}W_{q^l/q} = q^{(l-1)/2}\widehat{D}$$

in $\mathbb{Z}[\mathbb{F}_{q^l}^/\mathbb{F}_q^*]$;*

- (iii) *$D^{(-1)}W_{q^l/q}$ is divisible by $q^{(l-1)/2}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$.*

For example, when $D = \mathbb{F}_{q^l}^*/\mathbb{F}_q^*$, one obtains the classical Paley group scheme $S_{\mathbb{F}_{q^l}}$ in \mathbb{F}_{q^l} . In this case, the element \widehat{D} is either D or $-D$ depending on the value of the sum of coefficients of the Singer weighing matrix $W_{q^l/q}$. For each element D with ± 1 coefficients in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$, there are two subsets D_+ and D_- in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ such that $D_+ + D_- = \mathbb{F}_{q^l}^*/\mathbb{F}_q^*$, $D_+ - D_- = D$, and by equation (2), $(\tilde{\eta}_{\mathbb{F}_q^*} \circ \mu)^{-1}(D) = \mathbb{D}(D_+)$. Since $D^{(-1)}W_{q^l/q}$ is divisible by $q^{(l-1)/2}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$ if and only if $D_+^{(-1)}W_{q^l/q}$ is divisible by $q^{(l-1)/2}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$, and D is a projective half-point set in $\mathbb{F}_{q^l}^*$ over \mathbb{F}_q^* if and only if $D = \mathbb{D}(X)$ for some subset X in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ when l is odd, we have

Theorem 3.8. *Let l be odd and X be a subset of $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$. Then $\mathbb{D}(X)$ is a Paley type group scheme in \mathbb{F}_{q^l} if and only if $X^{(-1)}W_{q^l/q}$ is divisible by $q^{(l-1)/2}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$.*

Remark 3.9. For any odd integer l and any $S_{\mathbb{F}_q}$ invariant Paley type group scheme \mathbb{D} in \mathbb{F}_{q^l} , the set X is actually given by $X = \gamma(\mathbb{D} \cap S_{\mathbb{F}_{q^l}})$ and $\mathbb{D} = \mathbb{D}(X)$, where $\gamma : \mathbb{F}_{q^l}^* \rightarrow \mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ is the natural projection. It measures how much \mathbb{D} remains the same as or how much \mathbb{D} deviates from the standard Paley group schemes $S_{\mathbb{F}_{q^l}}$ and $N_{\mathbb{F}_{q^l}}$ in \mathbb{F}_{q^l} .

4. PROOFS OF THEOREMS 1.2–1.4

In order to prove Theorems 1.2–1.4, we need to use Gauss sums over finite fields because they are related to the character sums of Singer difference sets and Singer weighing matrices. Let ξ_p be a primitive p -th root of unity in the complex number field \mathbb{C} . For each character $\chi \in \widehat{\mathbb{F}_q^*}$, the Gauss sum $G_{\mathbb{F}_q}(\chi)$ of χ over \mathbb{F}_q is defined to be

$$G_{\mathbb{F}_q}(\chi) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \xi_p^{\text{tr}_{q/p}(x)}.$$

In [44], Yamamoto proved the following lemma.

Lemma 4.1. [44] *For the Singer difference set $S_{q^l/q}$ in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$, we have*

$$\chi(S_{q^l/q}) = -\frac{G_{\mathbb{F}_{q^l}}(\chi)}{q}$$

for each non-principal character $\chi \in \widehat{\mathbb{F}_{q^l}^*/\mathbb{F}_q^*}$.

Let $\chi \in \widehat{\mathbb{F}_{q^l}^*/\mathbb{F}_q^*}$ and $\eta_{\mathbb{F}_{q^l}^*}$ be the quadratic character of $\mathbb{F}_{q^l}^*$. Since l is odd, the restriction $\eta_{\mathbb{F}_{q^l}^*}|_{\mathbb{F}_q^*} = \eta_{\mathbb{F}_q^*}$. Therefore the Gauss sum

$$\begin{aligned} G_{\mathbb{F}_{q^l}}(\chi\eta_{\mathbb{F}_{q^l}^*}) &= \sum_{x \in \mathbb{F}_{q^l}^*} \xi_p^{\text{tr}_{q^l/p}(x)} (\chi\eta_{\mathbb{F}_{q^l}^*})(x) \\ &= \sum_{x \in \mathbb{F}_{q^l}^*} \xi_p^{\text{tr}_{q/p}(\text{tr}_{q^l/q}(x))} \chi(x)\eta_{\mathbb{F}_{q^l}^*}(x) \\ &= \sum_{x \in H^*} \xi_p^{\text{tr}_{q/p}(\text{tr}_{q^l/q}(x))} \chi(x)\eta_{\mathbb{F}_{q^l}^*}(x) + \sum_{x \in \mathbb{F}_q^*} \sum_{y \in S_{q^l/q}} \xi_p^{\text{tr}_{q/p}(\text{tr}_{q^l/q}(xy))} \chi(xy)\eta_{\mathbb{F}_{q^l}^*}(xy) \\ &= \sum_{x \in H^*} \chi(x)\eta_{\mathbb{F}_{q^l}^*}(x) + \sum_{x \in \mathbb{F}_q^*} \sum_{y \in S_{q^l/q}} \xi_p^{\text{tr}_{q/p}(x)} \eta_{\mathbb{F}_q^*}(x) \chi(y)\eta_{\mathbb{F}_{q^l}^*}(y) \\ &= G_{\mathbb{F}_q}(\eta_{\mathbb{F}_q^*})(\chi\eta_{\mathbb{F}_{q^l}^*})(S_{q^l/q}) \\ &= G_{\mathbb{F}_q}(\eta_{\mathbb{F}_q^*})\chi(W_{q^l/q}), \end{aligned}$$

where $H^* = \{x \in \mathbb{F}_{q^l}^* \mid \text{tr}_{q^l/q}(x) = 0\}$ as in the proof of Theorem 3.2. By the Davenport-Hasse product formula (see [8]) and Lemma 4.1, we have

$$G_{\mathbb{F}_{q^l}}(\chi\eta_{\mathbb{F}_{q^l}^*}) = \frac{G_{\mathbb{F}_{q^l}}(\chi^2)G_{\mathbb{F}_{q^l}}(\eta_{\mathbb{F}_{q^l}^*})}{\chi(2)^2 G_{\mathbb{F}_{q^l}}(\chi)}$$

and

$$\chi(W_{q^l/q}) = \frac{G_{\mathbb{F}_{q^l}}(\chi\eta_{\mathbb{F}_{q^l}^*})}{G_{\mathbb{F}_q}(\eta_{\mathbb{F}_q^*})} = \chi(4^{-1}) \frac{G_{\mathbb{F}_{q^l}}(\eta_{\mathbb{F}_{q^l}^*})}{G_{\mathbb{F}_q}(\eta_{\mathbb{F}_q^*})} \frac{G_{\mathbb{F}_{q^l}}(\chi^2)}{G_{\mathbb{F}_{q^l}}(\chi)} = \pm \chi(4^{-1}) q^{\frac{l-1}{2}} \frac{\chi(S_{q^l/q}^{(2)})}{\chi(S_{q^l/q})}.$$

Hence Theorem 3.8 can now be restated by using characters of $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$.

Theorem 4.2. *Let l be odd and X be a subset of $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$. Then $\mathbb{D}(X)$ is a Paley type group scheme in \mathbb{F}_{q^l} if and only if $\chi(S_{q^l/q}^{(2)})$ divides $\chi(X)\chi(S_{q^l/q})$ for all non-principal $\chi \in \widehat{\mathbb{F}_{q^l}^*/\mathbb{F}_q^*}$.*

Proof. By Theorem 3.8, $\mathbb{D}(X)$ is a Paley type group scheme in \mathbb{F}_{q^l} if and only if $X^{(-1)}W_{q^l/q}$ is divisible by $q^{(l-1)/2}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$. By the Fourier inversion formula, $X^{(-1)}W_{q^l/q}$ is divisible by $q^{(l-1)/2}$ in $\mathbb{Z}[\mathbb{F}_{q^l}^*/\mathbb{F}_q^*]$ if and only if $q^{(l-1)/2}$ divides $\chi(X^{(-1)})\chi(W_{q^l/q})$ for every $\chi \in \widehat{\mathbb{F}_{q^l}^*/\mathbb{F}_q^*}$, as $q^{(l-1)/2}$ is prime to $(q^l - 1)/(q - 1)$. From $\chi(W_{q^l/q}) = \pm \chi(4^{-1}) q^{\frac{l-1}{2}} \chi(S_{q^l/q}^{(2)})/\chi(S_{q^l/q})$ and $\chi(S_{q^l/q})\chi(S_{q^l/q}^{(-1)}) = \chi(S_{q^l/q}^{(2)})\chi(S_{q^l/q}^{(-2)})$, we find that $q^{(l-1)/2}$ divides $\chi(X^{(-1)})\chi(W_{q^l/q})$ if and only if $\chi(X)\chi(S_{q^l/q})$ is divisible by $\chi(S_{q^l/q}^{(2)})$ for all $\chi \in \widehat{\mathbb{F}_{q^l}^*/\mathbb{F}_q^*}$. \square

As an application of Theorem 4.2, we give a new proof of Theorem 3.6 and Corollary 3.7 in [26], which slightly generalizes these results. These results themselves are generalizations of Theorem 3.6 in [27]. To this end, we need the following proposition of Langevin [31].

Proposition 4.3. [31, Proposition 4.2] *Let m be a positive integer and $p' \neq 3$ be a prime such that $p' \equiv 3 \pmod{8}$ and the order l of p in $\mathbb{Z}_{p'^m}^*$ is $l = (p'^m - p'^{m-1})/2$. Let $q = p^l$ and $\chi \in \widehat{\mathbb{F}_q^*/\mathbb{F}_p^*}$ such that the order of χ is p'^m . Then*

$$G_{\mathbb{F}_q}(\chi) = p^{\frac{l-h}{2}} \frac{a + b\sqrt{-p'}}{2},$$

where h is the class number of $\mathbb{Q}(\sqrt{-p'})$ and a and b are integers such that

- (i) p does not divide b ,
- (ii) $a \equiv -2p^{(l+h)/2} \pmod{p'}$,
- (iii) $a^2 + b^2p' = 4p^h$.

Items (i) and (ii) imply that $ab \neq 0$. Therefore when $4p^h = 1 + p'$, the Gauss sum

$$G_{\mathbb{F}_q}(\chi) = p^{\frac{l-h}{2}} \frac{\pm 1 \pm \sqrt{-p'}}{2}.$$

Since $\frac{\pm 1 \pm \sqrt{-p'}}{2} \in \{\chi'(S_{\mathbb{F}_{p'}}), \chi'(N_{\mathbb{F}_{p'}}), \chi'(S_{\mathbb{F}_{p'}} \cup \{0\}), \chi'(N_{\mathbb{F}_{p'}} \cup \{0\})\}$ for every non-principal character χ' of the additive group of $\mathbb{F}_{p'}$, and p generates $S_{\mathbb{F}_{p'}}$ as the order of p in $\mathbb{Z}_{p'^m}^*$ is $(p'^m - p'^{m-1})/2$, Lemma 4.1 and Proposition 4.3 imply the following corollary.

Corollary 4.4. *Let m be a positive integer and $p' \neq 3$ be a prime such that $p' \equiv 3 \pmod{8}$, the order l of p in $\mathbb{Z}_{p'^m}^*$ is $l = (p'^m - p'^{m-1})/2$ and $4p^h = 1 + p'$, where h is the class number of $\mathbb{Q}(\sqrt{-p'})$. Let $q = p^l$. If we identify the subgroup of order p' in $\mathbb{Z}_{p'^m}$ with $\mathbb{F}_{p'}$, then there is a unique subset $P_{q/p} \in \{S_{\mathbb{F}_{p'}}, N_{\mathbb{F}_{p'}}, S_{\mathbb{F}_{p'}} \cup \{0\}, N_{\mathbb{F}_{p'}} \cup \{0\}\}$ in $\mathbb{F}_{p'}$ such that for every $\chi \in \widehat{\mathbb{F}_q^*/\mathbb{F}_p^*}$ of order p'^m ,*

$$\chi(S_{q/p}) = -p^{\frac{l-h-2}{2}} \chi(P_{q/p}).$$

Corollary 4.4 yields the following theorem which is slightly more general than Theorem 3.6 and Corollary 3.7 in [26] because our T in the theorem is an arbitrary transversal.

Theorem 4.5. *Let m be a positive integer and $p' \neq 3$ be a prime such that $p' \equiv 3 \pmod{8}$, the order l of p in $\mathbb{Z}_{p'^m}^*$ is $l = (p'^m - p'^{m-1})/2$ and $4p^h = 1 + p'$, where h is the class number of $\mathbb{Q}(\sqrt{-p'})$. Let $q = p^l$ and $\gamma : \mathbb{F}_q/\mathbb{F}_p \rightarrow \mathbb{Z}_{p'^m}$ be the natural projection. Let $P_{q/p}$ be the subset in the subgroup of order p' in $\mathbb{Z}_{p'^m}$ as in Corollary 4.4. Then for every transversal T of the subgroup of order p' in $\mathbb{Z}_{p'^m}$, $TP_{q/p}^{(2)}$ is a subset in $\mathbb{Z}_{p'^m}$ and $\mathbb{D}(\gamma^{-1}(TP_{q/p}^{(2)}))$ is a Paley type group scheme in \mathbb{F}_q .*

Proof. Let χ be a non-principal character of $\mathbb{F}_q^*/\mathbb{F}_p^*$. If χ is non-principal on the kernel of γ , then $\chi(\gamma^{-1}(TP_{q/p}^{(2)}))\chi(S_{q/p}) = 0$ and $\chi(S_{q/p}^{(2)})$ divides $\chi(\gamma^{-1}(TP_{q/p}^{(2)}))\chi(S_{q/p})$. If χ is principal on the kernel of γ , then $\chi \in \widehat{\mathbb{Z}_{p'^m}}$. If χ has order p'^m , then by Corollary 4.4, we have that the character sum $\chi(S_{q/p}^{(2)}) = \chi^2(S_{q/p}) = -p^{\frac{l-h-2}{2}} \chi^2(P_{q/p}) = -p^{\frac{l-h-2}{2}} \chi(P_{q/p}^{(2)})$ divides

$$\chi(\gamma^{-1}(TP_{q/p}^{(2)}))\chi(S_{q/p}) = -p^{\frac{l-h-2}{2}} |\text{Ker}(\gamma)| \chi(T) \chi(P_{q/p}^{(2)}) \chi(P_{q/p}).$$

If χ has order dividing p'^m but not equal to p'^m , then $\chi(T) = 0$ as T is a transversal of the subgroup of order p' in $\mathbb{Z}_{p'^m}$. Hence $\chi(S_{q/p}^{(2)})$ divides $\chi(\gamma^{-1}(TP_{q/p}^{(2)}))\chi(S_{q/p}) = 0$. By Theorem 4.2, $\mathbb{D}(\gamma^{-1}(TP_{q/p}^{(2)}))$ is a Paley type group scheme in \mathbb{F}_q . \square

We now prove Theorems 1.2–1.4.

Proof of Theorem 1.2: Let X be a $((q^l - 1)/(q - 1), q^{l-1}, q^{l-2}(q - 1))$ -difference set in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$. If $\mathbb{D}(X)$ is a Paley type group scheme in \mathbb{F}_{q^l} , then by Theorem 4.2, $\chi(S_{q^l/q}^{(2)})$ divides $\chi(X)\chi(S_{q^l/q})$ for every $\chi \in \widehat{\mathbb{F}_{q^l}^*/\mathbb{F}_q^*}$, and therefore q^{l-2} divides $\chi(X)\chi(S_{q^l/q})\chi(S_{q^l/q}^{(-2)})$, or equivalently, q^{l-2} divides

$\chi(X^{(-1)})\chi(S_{q^l/q}^{(-1)})\chi(S_{q^l/q}^{(2)})$ for every $\chi \in \widehat{\mathbb{F}_{q^l}^*/\mathbb{F}_q^*}$. By the Fourier inversion formula and Theorem 2.3, there is a $((q^l - 1)/(q - 1), q^{l-1}, q^{l-2}(q - 1))$ -difference set Y in $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ such that

$$X^{(-1)}S_{q^l/q}^{(-1)}S_{q^l/q}^{(2)} = (q^{l-2} + (q^{l-1} - q^{l-2})\mathbb{F}_{q^l}^*/\mathbb{F}_q^*)Y.$$

This implies that $XY = S_{q^l/q}^{(-1)}S_{q^l/q}^{(2)}$ and X is an Arasu-Dillon-Player difference set.

Conversely, if X is an Arasu-Dillon-Player difference set, then by Remark 2.6, $S_{q^l/q}^{(2)}$ divides $XS_{q^l/q}$, and therefore $\chi(S_{q^l/q}^{(2)})$ divides $\chi(X)\chi(S_{q^l/q})$ for every $\chi \in \widehat{\mathbb{F}_{q^l}^*/\mathbb{F}_q^*}$. By Theorem 4.2, $\mathbb{D}(X)$ is a Paley type group scheme in \mathbb{F}_{q^l} . \square

Proof of Theorem 1.3: Let χ be a non-principal character of $\mathbb{F}_{q^l}^*/\mathbb{F}_l^*$. If χ is non-principal on the kernel of γ , then $\chi(\gamma^{-1}(X))\chi(S_{q^l/q}) = 0$ and $\chi(S_{q^l/q}^{(2)})$ divides $\chi(\gamma^{-1}(X))\chi(S_{q^l/q})$. If χ is principal on the kernel of γ , then $\chi \in \widehat{\mathbb{Z}_n}$ and $\chi(S_{q^l/q}^{(2)}) = \chi^2(S_{q^l/q}) = \chi^{p^t}(S_{q^l/q}) = \chi(S_{q^l/q}^{(p^t)})$ for some integer t as $2 \in \langle p \rangle$ in \mathbb{Z}_n^* , and $\chi(S_{q^l/q}^{(2)}) = \chi(S_{q^l/q})$ as $p \in \mathcal{M}_0(S_{q^l/q})$. This again implies that $\chi(S_{q^l/q}^{(2)})$ divides $\chi(\gamma^{-1}(X))\chi(S_{q^l/q})$. By Theorem 4.2, $\mathbb{D}(\gamma^{-1}(X))$ is a Paley type group scheme in \mathbb{F}_{q^l} . \square

Proof of Theorem 1.4: If $\mathbb{D}(X)$ is a Paley type group scheme in \mathbb{F}_{q^t} , by Theorem 4.2, $\chi(S_{q^t/q}^{(2)})$ divides $\chi(X)\chi(S_{q^t/q})$ for all $\chi \in \widehat{\mathbb{F}_{q^t}^*/\mathbb{F}_q^*}$. By Gordon-Mills-Welch decomposition, $S_{q^{st}/q}^{(2)} = \tilde{R}_{q^{st}/q^t}^{(2)}S_{q^t/q}^{(2)}$ and $S_{q^{st}/q} = \tilde{R}_{q^{st}/q^t}S_{q^t/q}$. Therefore $\chi(S_{q^{st}/q}^{(2)}) = \chi(\tilde{R}_{q^{st}/q^t}^{(2)})\chi(S_{q^t/q}^{(2)})$ divides $\chi(\tilde{R}_{q^{st}/q^t}^{(2)})\chi(X)\chi(S_{q^t/q})$, which also divides $\chi(\tilde{R}_{q^{st}/q^t}^{(2)})\chi(X)\chi(\tilde{R}_{q^{st}/q^t})\chi(S_{q^t/q}) = \chi(\tilde{R}_{q^{st}/q^t}^{(2)}X)\chi(S_{q^{st}/q^t})$ for all $\chi \in \widehat{\mathbb{F}_{q^{st}}^*/\mathbb{F}_q^*}$. By Theorem 4.2, $\mathbb{D}(\tilde{R}_{q^{st}/q^t}^{(2)}X)$ is a Paley type group scheme in $\mathbb{F}_{q^{st}}$. Since $\tilde{R}_{q^{st}/q^t}^{(2)}\tilde{R}_{q^{st}/q^t}^{(-2)} = \tilde{R}_{q^{st}/q^t}\tilde{R}_{q^{st}/q^t}^{(-1)}$, $\chi(\tilde{R}_{q^{st}/q^t}^{(2)})$ divides $\chi(\tilde{R}_{q^{st}/q^t})\chi(\tilde{R}_{q^{st}/q^t}^{(-1)})$ for all $\chi \in \widehat{\mathbb{F}_{q^{st}}^*/\mathbb{F}_q^*}$. Therefore $\chi(S_{q^{st}/q}^{(2)}) = \chi(\tilde{R}_{q^{st}/q^t}^{(2)})\chi(S_{q^t/q}^{(2)})$ divides $\chi(\tilde{R}_{q^{st}/q^t})\chi(\tilde{R}_{q^{st}/q^t}^{(-1)})\chi(X)\chi(S_{q^t/q}) = \chi(\tilde{R}_{q^{st}/q^t}^{(-1)}X)\chi(S_{q^{st}/q})$ for all $\chi \in \widehat{\mathbb{F}_{q^{st}}^*/\mathbb{F}_q^*}$, and by Theorem 4.2, $\mathbb{D}(\tilde{R}_{q^{st}/q^t}^{(-1)}X)$ is a Paley type group scheme in $\mathbb{F}_{q^{st}}$. \square

5. CONCLUSIONS

In \mathbb{F}_{5^3} , the Paley type group scheme $\mathbb{D}(S_{5^3/5}^{(2)})$ has $|\text{Aut}(\mathfrak{C}(\mathbb{D}(S_{5^3/5}^{(2)})))| = 2^3 \cdot 3 \cdot 5^3$ and Theorem 1.2 replaces one of the question marks in Table 1.

Using Theorem 2.7 and Theorem 1.2, we did a MAGMA search and found the following 10 inequivalent Paley type group schemes in \mathbb{F}_{3^5} which have non-isomorphic configurations: $\mathbb{D}(S_{3^5/3}^{(2)})$, $\mathbb{D}(S_{3^5/3}^{(4)})$, $\mathbb{D}(S_{3^5/3}^{(5)})$, $\mathbb{D}(S_{3^5/3}^{(10)})$, $\mathbb{D}(S_{3^5/3}^{(20)})$, $\mathbb{D}(S_{3^5/3}^{(40)})$, $\mathbb{D}(A_{3^5/3}(4))$, $\mathbb{D}(A_{3^5/3}(5))$, $\mathbb{D}(A_{3^5/3}(10))$, $\mathbb{D}(A_{3^5/3}(20))$. These Paley type group schemes are all $\text{Gal}(\mathbb{F}_{3^5})$ invariant and none of them is equivalent to the Paley type group scheme from the 3 semifields mentioned in [18]. The scheme $\mathbb{D}(S_{3^5/3}^{(10)})$ is equivalent to $\text{RT}(1)$ while $\mathbb{D}(A_{3^5/3}(10))$ is equivalent to $\text{RT}(-1)$ (see [23]). Theorem 3.8 or Theorem 4.2 clearly has the following consequence.

Theorem 5.1. *Let l be an odd integer and X_1 and X_2 be subsets of $\mathbb{F}_{q^l}^*/\mathbb{F}_q^*$. If $X_1 \cap X_2 = \emptyset$ and $\mathbb{D}(X_1)$ and $\mathbb{D}(X_2)$ are both Paley type group schemes in \mathbb{F}_{q^l} , then $\mathbb{D}(X_1 \cup X_2)$ is also a Paley type group scheme in \mathbb{F}_{q^l} . Equivalently, If $X_1 \cup X_2 = \mathbb{F}_{q^l}^*/\mathbb{F}_q^*$ and $\mathbb{D}(X_1)$ and $\mathbb{D}(X_2)$ are both Paley type group schemes in \mathbb{F}_{q^l} , then $\mathbb{D}(X_1 \cap X_2)$ is also a Paley type group scheme in \mathbb{F}_{q^l} .*

Among the 10 Arasu-Dillon-Player difference sets we used in $\mathbb{F}_{3^5}^*/\mathbb{F}_3^*$, we found that $S_{3^5/3}^{(5)} \cup A_{3^5/3}(5) = \mathbb{F}_{3^5}^*/\mathbb{F}_3^*$ and, by Theorem 5.1, $\mathbb{D}(S_{3^5/3}^{(5)} \cap A_{3^5/3}(5))$ is a Paley type group scheme, whose configuration

is not isomorphic to any of the configurations of the aforementioned 13 Paley type group schemes in \mathbb{F}_{35} . We now understand how to construct 14 of the 58 $\text{Gal}(\mathbb{F}_{35})$ invariant Paley type group schemes in Table 2 and still have 44 more to go.

In \mathbb{F}_{73} , Theorem 1.2 yields two non-isomorphic configurations from $\mathbb{D}(S_{73/7}^{(2)})$ and $\mathbb{D}(S_{73/7}^{(-1)})$ and these two Paley type group schemes have

$$|\text{Aut}(\mathfrak{C}(\mathbb{D}(S_{73/7}^{(2)})))| = |\text{Aut}(\mathfrak{C}(\mathbb{D}(S_{73/7}^{(-1)})))| = 3^2 \cdot 7^3.$$

In \mathbb{F}_{37} , we used a MAGMA program and found that $\mathbb{D}(S_{37/3}^{(2)})$, $\mathbb{D}(S_{37/3}^{(4)})$, $\mathbb{D}(S_{37/3}^{(5)})$, $\mathbb{D}(S_{37/3}^{(10)})$, $\mathbb{D}(S_{37/3}^{(14)})$, $\mathbb{D}(S_{37/3}^{(28)})$, $\mathbb{D}(S_{37/3}^{(182)})$, $\mathbb{D}(S_{37/3}^{(364)})$, $\mathbb{D}(A_{37/3}(4))$, $\mathbb{D}(A_{37/3}(5))$, $\mathbb{D}(A_{37/3}(10))$, $\mathbb{D}(A_{37/3}(14))$, $\mathbb{D}(A_{37/3}(28))$ and $\mathbb{D}(A_{37/3}(182))$ are all the inequivalent Paley type group schemes with non-isomorphic configurations that can be obtained from Theorem 1.2 and Theorem 2.7. None of the configurations of these Paley type group schemes is isomorphic to that of $\text{DY}(1)$, $\text{DY}(-1)$, $\text{RT}(1)$ or $\text{RT}(-1)$, where $\text{DY}(\pm 1)$ are the Paley type group schemes constructed in [24] and $\text{RT}(\pm 1)$ are those in [23]. Therefore, besides Paley group scheme, there are at least 18 $\text{Gal}(\mathbb{F}_{37})$ invariant Paley type group schemes with non-isomorphic configurations in \mathbb{F}_{37} .

Acknowledgement: Y. Q. Chen would like to thank the Department of Mathematics at Zhejiang University for the hospitality he received during his visit when this research was initiated. The work of T. Feng was supported in part by the Fundamental Research Funds for the Central Universities, Zhejiang Provincial Natural Science Foundation.

REFERENCES

- [1] K. T. Arasu, Sequences and arrays with desirable correlation properties, <http://www.math.uniri.hr/NATO-ASI/abstracts/arasu.pdf>
- [2] K. T. Arasu, A reduction theorem for circulant weighing matrices, *Australas. J. Combin.* **18** (1998), 111–114.
- [3] K. T. Arasu, Y. Q. Chen, J. F. Dillon, X. Liu and K. J. Player, Abelian difference sets of order n dividing λ , *Des. Codes Cryptogr.* **44** (2007), 307–319.
- [4] K. T. Arasu, J. F. Dillon, and K. J. Player, Character Sum Factorizations Yield Perfect Sequences, (Preprint).
- [5] K. T. Arasu, K. H. Leung, S. L. Ma, A. Nabavi, and D. K. Ray-Chaudhuri, Determination of all possible orders of weight 16 circulant weighing matrices, *Finite Fields Appl.* **12** (2006), 498–538.
- [6] K. T. Arasu, K. H. Leung, S. L. Ma, A. Nabavi, and D. K. Ray-Chaudhuri, Circulant weighing matrices of weight 2^{2t} , *Des. Codes Cryptogr.* **41** (2006), 111–123.
- [7] K. T. Arasu, and S. L. Ma, Some new results on circulant weighing matrices. *J. Algebraic Combin.* **14** (2001), 91–101.
- [8] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998.
- [9] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, volume 1. Cambridge University Press, Cambridge, 2nd edition, 1999.
- [10] L. Carlitz, A theorem on permutations in a finite field. *Proc. Amer. Math. Soc.* **11** (1960) 456–459.
- [11] P. Camion and H.B. Mann, Antisymmetric difference sets, *J. Number Theory* **4** (1972) 266–268.
- [12] Y. Q. Chen, Divisible designs and semi-regular relative difference sets from additive Hadamard cocycles, *J. Combin. Theory Ser. A* **118** (2011), 2185–2206.
- [13] Y. Q. Chen, Multiplicative characterization of some difference sets in elementary abelian groups, *J. Comb. Inf. Syst. Sci.* **34** (2009), 95–111.
- [14] Y. Q. Chen, On the existence of abelian Hadamard difference sets and a new family of difference sets, *Finite Fields Appl.* **3** (1997), 234–256.
- [15] Y. Q. Chen, Q. Xiang, and S. K. Sehgal, An exponent bound on skew Hadamard abelian difference sets, *Des. Codes Cryptogr.* **4** (1994), 313–317.
- [16] Y. Q. Chen and T. Feng, Abelian and non-abelian Paley type group schemes, *Des. Codes Cryptogr.* (to appear)
- [17] Y. Q. Chen and J. Polhill, Paley type group schemes and planar Dembowski-Ostrom polynomials, *Discrete Math.* **311** (2011), 1349–1364.
- [18] R. Coulter, and P. Kosick, Commutative semifields of order 243 and 3125. *Finite fields: theory and applications*, Contemp. Math., **518**, Amer. Math. Soc., Providence, RI, (2010) 129–136.

- [19] J. A. Davis, Partial difference sets in p -groups, *Arch. Math.* **63** (1994), 103–110.
- [20] J. F. Dillon, Elementary Hadamard difference sets, PhD thesis, University of Maryland (1974).
- [21] J. F. Dillon, Elementary Hadamard difference sets. Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing (1975), 237–249. Congressus Numerantium, No. XIV, Utilitas Math., Winnipeg, Man., 1975.
- [22] J. F. Dillon, Multiplicative difference sets via additive characters, *Des. codes Cryptogr.* **17** (1999), 225–235.
- [23] C. Ding, Z. Wang and Q. Xiang, Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in $\text{PG}(3, 3^{2h+1})$, *J. Combin. Theory Ser. A* **114** (2007), 867–887.
- [24] C. Ding and J. Yin, A family of skew Hadamard difference sets, *J. Combin. Theory Ser. A* **113** (2006), 1526–1535.
- [25] T. Feng, Non-abelian skew Hadamard difference sets fixed by a prescribed automorphism, *J. Combin. Theory Ser. A* **118** (2011), 27–36.
- [26] T. Feng, K. Momihara and Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, arXiv:1206.3354
- [27] T. Feng and Q. Xiang, Cyclotomic constructions of skew Hadamard difference sets, *J. Combin. Theory Ser. A* **119** (2012), 245–256.
- [28] B. Gordon, W. H. Mills and L. R. Welch, Some new difference sets, *Canad. J. Math.* **14** (1962) 614–625.
- [29] E. C. Johnson, Skew-Hadamard abelian group difference sets, *J. Algebra* **4** (1966) 388–402.
- [30] W. M. Kantor, 2-transitive symmetric designs, *Trans. Amer. Math. Soc.* **146** (1969) 1–28.
- [31] P. Langevin, Calculus de certaines sommes de Gauss, *J. Number Theory* **63** (1997), 59–64.
- [32] K. H. Leung, S. L. Ma, and B. Schmidt, Constructions of relative difference sets with classical parameters and circulant weighing matrices, *J. Combin. Theory Ser. A* **99** (2002), 111–127.
- [33] A. Lubotzky, R. Phillips and P. Sarnak, Ramanujan Graphs, *Combinatorica* **8** (1988), 261–277.
- [34] S. L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.* **4** (1994), 221–261.
- [35] S. L. Ma, Reversible Relative Difference Sets, *Combinatorica* **12** (1992) 425–432.
- [36] M. Muzychuk, On skew Hadamard difference sets, arXiv:1012.2089v1
- [37] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933), 311–320.
- [38] W. Peisert, All self-complementary symmetric graphs, *J. Algebra* **240** (2001), 209–229,
- [39] J. Polhill, Paley type partial difference sets in non p -groups, *Des. Codes Cryptogr.* **52** (2009), 163–169.
- [40] J. Polhill, Paley type partial difference sets in groups of order n^4 and $9n^4$ for any odd n , *J. Combin. Theory Ser. A* **117** (2010), 1027–1036.
- [41] A. Pott, *Finite geometry and character theory*, Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin, Heidelberg, 1995.
- [42] G. Weng, W. Qiu, Z. Wang and Q. Xiang, Pseudo-Paley graphs and skew Hadamard difference sets from presemifields, *Des. Codes Cryptogr.* **44** (2007), 49–62.
- [43] Q. Xiang, Note on Paley type partial difference sets, *Groups, difference sets, and the Monster* (Columbus, OH, 1993), Ohio State Univ. Math. Res. Inst. Publ., 4, de Gruyter, Berlin, 1996, 239–244.
- [44] K. Yamamoto, On congruences arising from relative Gauss sum, in *Number Theory and Combinatorics*, 423–446, World Scientific, Singapore, 1955.

DEPARTMENT OF MATHEMATICS AND STATISTICS, WRIGHT STATE UNIVERSITY, DAYTON, OH 45435

E-mail address: `yuqing.chen@wright.edu`

DEPARTMENT OF MATHEMATICS, ZHEJIANG UNIVERSITY, HANGZHOU 310027, CHINA

E-mail address: `tfeng@zju.edu.cn`